Recent Developments in Asymptotically Good Quantum LDPC Codes

Eugene Tang

DYNISQ22 – KITP

September 13, 2022

What are Quantum LDPC Codes and Why Should We Care?

- Low-Density Parity Check (LDPC) codes are error-correcting codes with very succinct descriptions. .

What are Quantum LDPC Codes and Why Should We Care?

- Low-Density Parity Check (LDPC) codes are error-correcting codes with very succinct descriptions. *Efficient codes*.

What are Quantum LDPC Codes and Why Should We Care?

- Low-Density Parity Check (LDPC) codes are error-correcting codes with very succinct descriptions. *Efficient codes*.
- Classical LDPC codes are the *gold standard* in error-correction.

What are Quantum LDPC Codes and Why Should We Care?

- Low-Density Parity Check (LDPC) codes are error-correcting codes with very succinct descriptions. *Efficient codes*.
- Classical LDPC codes are the *gold standard* in error-correction.
- Efficient quantum LDPC codes are expected to have good fault-tolerant properties [G13].

What are Quantum LDPC Codes and Why Should We Care?

- Low-Density Parity Check (LDPC) codes are error-correcting codes with very succinct descriptions. *Efficient codes*.
- Classical LDPC codes are the *gold standard* in error-correction.
- Efficient quantum LDPC codes are expected to have good fault-tolerant properties [G13].
- Deep connections to many-body physics and complexity theory [DELLM21, HL22, ABN22].

What are Quantum LDPC Codes and Why Should We Care?

- Low-Density Parity Check (LDPC) codes are error-correcting codes with very succinct descriptions. *Efficient codes*.
- Classical LDPC codes are the *gold standard* in error-correction.
- Efficient quantum LDPC codes are expected to have good fault-tolerant properties [G13].
- Deep connections to many-body physics and complexity theory [DELLM21, HL22, ABN22].
- Most of the quantum codes we care about are in fact LDPC. The toric code, for example.

What are Quantum LDPC Codes and Why Should We Care?

- Low-Density Parity Check (LDPC) codes are error-correcting codes with very succinct descriptions. *Efficient codes*.
- Classical LDPC codes are the *gold standard* in error-correction.
- Efficient quantum LDPC codes are expected to have good fault-tolerant properties [G13].
- Deep connections to many-body physics and complexity theory [DELLM21, HL22, ABN22].
- Most of the quantum codes we care about are in fact LDPC. The toric code, for example. Our focus will be on *good* codes.

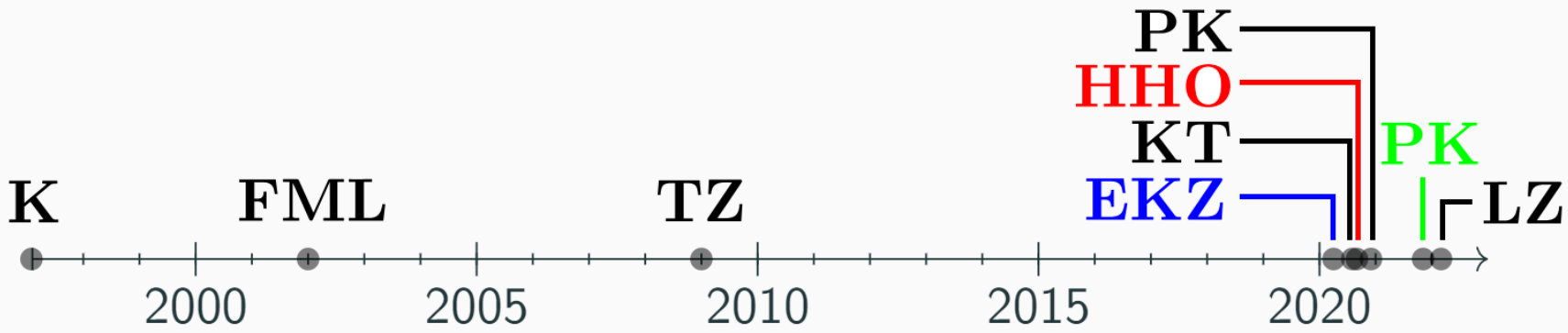
What are Quantum LDPC Codes and Why Should We Care?

- Low-Density Parity Check (LDPC) codes are error-correcting codes with very succinct descriptions. *Efficient codes*.
- Classical LDPC codes are the *gold standard* in error-correction.
- Efficient quantum LDPC codes are expected to have good fault-tolerant properties [G13].
- Deep connections to many-body physics and complexity theory [DELLM21, HL22, ABN22].
- Most of the quantum codes we care about are in fact LDPC. The toric code, for example. Our focus will be on *good* codes.

What is the fundamental limitation to efficient quantum information storage?

The Quantum LDPC Progression

k	d	Name
2	$\sqrt{n\sqrt{\log n}}$	Freedman-Meyer-Luo
n	$\sqrt{n}$	Tillich-Zémor
n	$\sqrt{n}\log n$	Evra–Kaufman–Zémor
$\sqrt{n}$	$\sqrt{n}\log^c n$	Kaufman-Tessler
$n^{3/5}/\mathrm{polylog}n$	$n^{3/5}/\mathrm{polylog}n$	Haah-Hastings-O'Donnell
$\log n$	$n/\log n$	Panteleev-Kalachev
$\Theta(n)$	$\Theta(n)$	Panteleev-Kalachev
$\Theta(n)$	$\Theta(n)$	Leverrier-Zémor



Classical LDPC Codes

A classical error correcting code is a subspace $C \subseteq \mathbb{F}_2^n$.

Classical LDPC Codes

A classical error correcting code is a subspace $C \subseteq \mathbb{F}_2^n$. Specified by a *parity check* matrix H such that $C = \ker H$. If $\operatorname{rank} H = n - k$ then C encodes k logical bits into n physical bits.

Classical LDPC Codes

A classical error correcting code is a subspace $C \subseteq \mathbb{F}_2^n$. Specified by a *parity check* matrix H such that $C = \ker H$. If $\operatorname{rank} H = n - k$ then C encodes k logical bits into n physical bits. The *distance* d of the code is defined by

$$d = \min_{\substack{x,y \in C \\ x \neq y}} |x - y| = \min_{\substack{x \in C \\ x \neq 0}} |x|. \tag{1}$$

Classical LDPC Codes

A classical error correcting code is a subspace $C \subseteq \mathbb{F}_2^n$. Specified by a *parity check* matrix H such that $C = \ker H$. If $\operatorname{rank} H = n - k$ then C encodes k logical bits into n physical bits. The *distance* d of the code is defined by

$$d = \min_{\substack{x,y \in C \\ x \neq y}} |x - y| = \min_{\substack{x \in C \\ x \neq 0}} |x|. \tag{1}$$

Given a code family $\mathcal{C} = \{C_n\}_{n \to \infty}$, we say that $\mathcal{C}$ is *asymptotically good* if $k = \Theta(n)$ and $d = \Theta(n)$.

Classical LDPC Codes

A classical error correcting code is a subspace $C \subseteq \mathbb{F}_2^n$. Specified by a *parity check* matrix H such that $C = \ker H$. If $\operatorname{rank} H = n - k$ then C encodes k logical bits into n physical bits. The *distance* d of the code is defined by

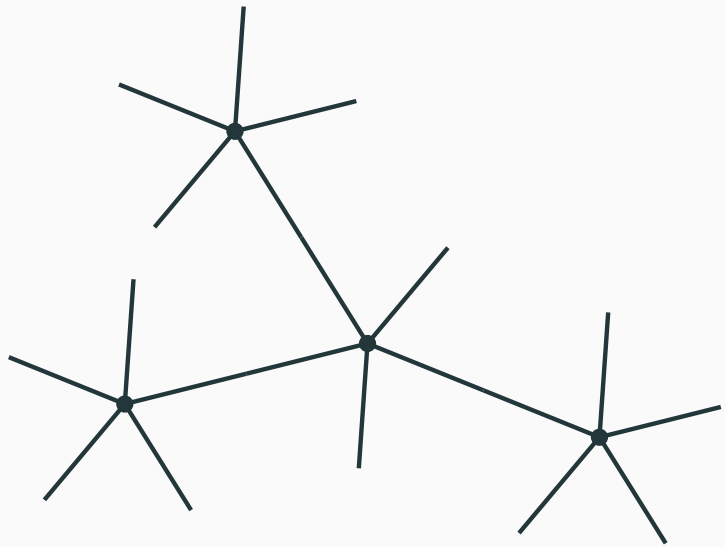
$$d = \min_{\substack{x,y \in C \\ x \neq y}} |x - y| = \min_{\substack{x \in C \\ x \neq 0}} |x|. \tag{1}$$

Given a code family $\mathcal{C} = \{C_n\}_{n \to \infty}$, we say that $\mathcal{C}$ is *asymptotically good* if $k = \Theta(n)$ and $d = \Theta(n)$.

The code family is *low-density parity check* (LDPC) if every row and column of H has $O(1)$ non-zero entries.

Classical Tanner Codes

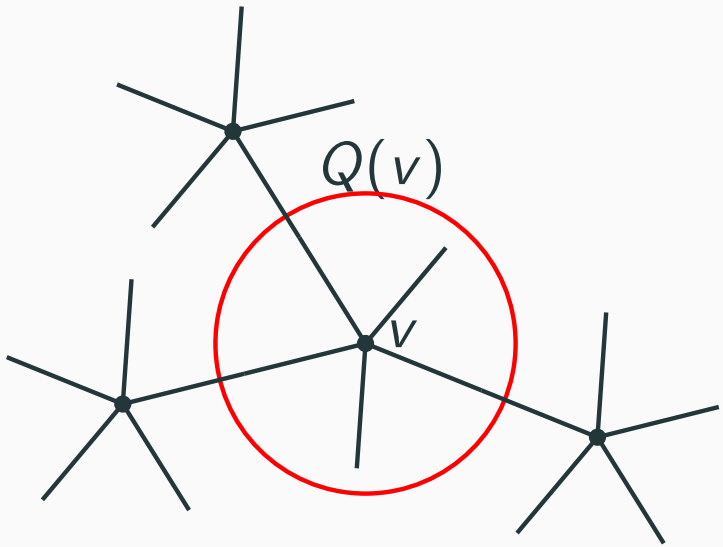
Take a Δ-regular expander graph $\Gamma = (V, E)$.



Classical Tanner Codes

Take a Δ-regular expander graph $\Gamma = (V, E)$.

Fix a *local (or base)* code C of blocklength Δ.

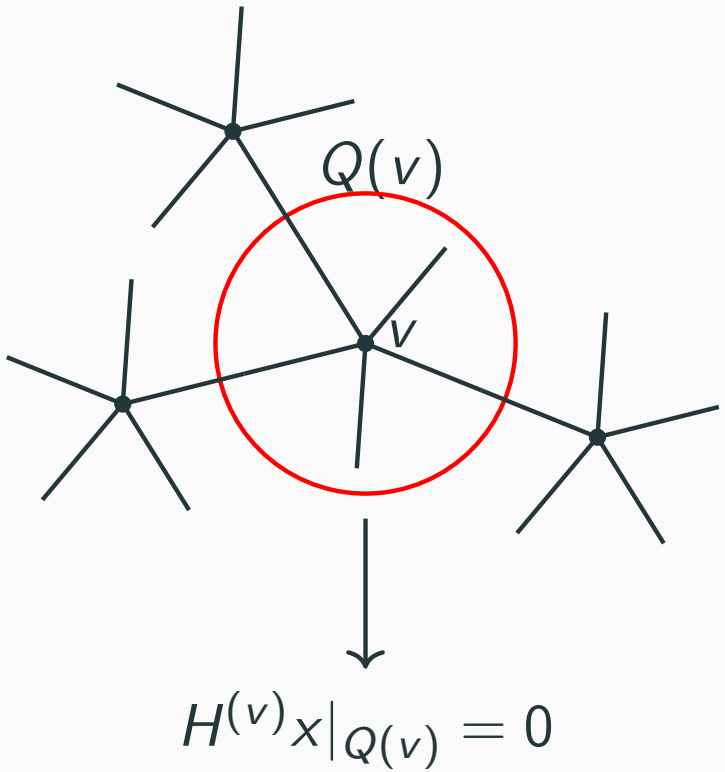


Classical Tanner Codes

Take a Δ-regular expander graph $\Gamma = (V, E)$.

Fix a *local (or base)* code C of blocklength Δ.

The *Tanner code* $T(\Gamma, C) \subseteq \mathbb{F}_2^E$ is defined with bits placed on the edges of Γ so that $x \in T$ if and only if $x|_{Q(v)} \in C$ for each vertex $v \in V$.



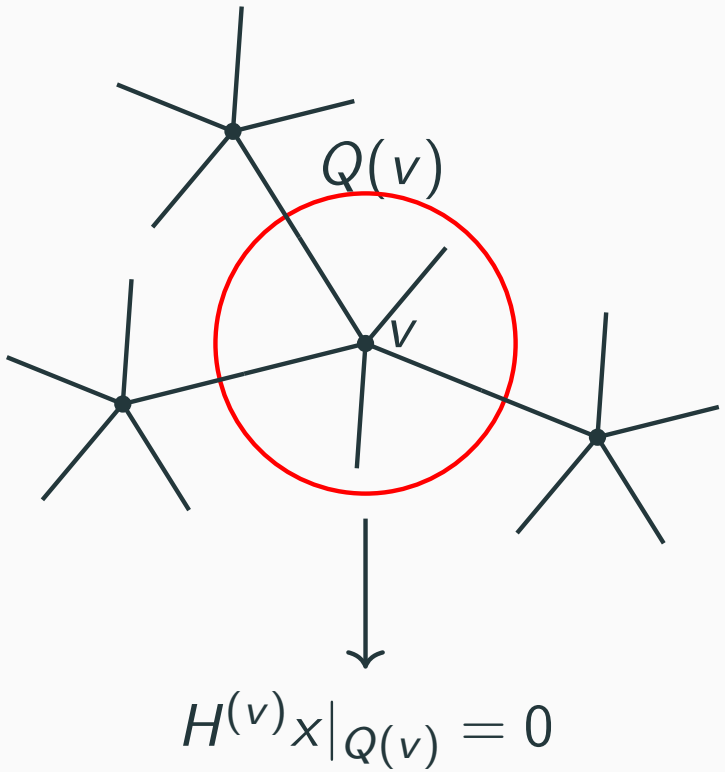
Classical Tanner Codes

Take a Δ-regular expander graph $\Gamma = (V, E)$.

Fix a *local (or base)* code C of blocklength Δ.

The *Tanner code* $T(\Gamma, C) \subseteq \mathbb{F}_2^E$ is defined with bits placed on the edges of Γ so that $x \in T$ if and only if $x|_{Q(v)} \in C$ for each vertex $v \in V$.

Efficiently decodable good classical LDPC code family [SS96].



Expansion and Amplification

Moral Definition: Expander graphs are graphs which *amplify* local properties into global properties.

Expansion and Amplification

Moral Definition: Expander graphs are graphs which *amplify* local properties into global properties.

Expander Mixing Lemma: Let $\Gamma = (V, E)$ be a Δ-regular λ-expander. Then for any $S, T \subseteq V$ we have

$$\left| E(S,T) - \frac{\Delta}{|V|}|S||T| \right| \leq \lambda\sqrt{|S||T|}. \tag{2}$$

Expansion and Amplification

Moral Definition: Expander graphs are graphs which *amplify* local properties into global properties.

Expander Mixing Lemma: Let $\Gamma = (V, E)$ be a Δ-regular λ-expander. Then for any $S, T \subseteq V$ we have

$$\left| E(S,T) - \frac{\Delta}{|V|}|S||T| \right| \leq \lambda\sqrt{|S||T|}. \tag{2}$$

Distance Amplification: Let $T(\Gamma, C)$ be a Tanner code with C having distance $\delta\Delta$.

Expansion and Amplification

Moral Definition: Expander graphs are graphs which *amplify* local properties into global properties.

Expander Mixing Lemma: Let $\Gamma = (V, E)$ be a Δ-regular λ-expander. Then for any $S, T \subseteq V$ we have

$$\left| E(S,T) - \frac{\Delta}{|V|}|S||T| \right| \leq \lambda\sqrt{|S||T|}. \tag{2}$$

Distance Amplification: Let $T(\Gamma, C)$ be a Tanner code with C having distance $\delta\Delta$.

1. A non-trivial codeword $x \in T$ induces a subgraph Γ'.

Expansion and Amplification

Moral Definition: Expander graphs are graphs which *amplify* local properties into global properties.

Expander Mixing Lemma: Let $\Gamma = (V, E)$ be a Δ-regular λ-expander. Then for any $S, T \subseteq V$ we have

$$\left| E(S,T) - \frac{\Delta}{|V|}|S||T| \right| \leq \lambda\sqrt{|S||T|}. \tag{2}$$

Distance Amplification: Let $T(\Gamma, C)$ be a Tanner code with C having distance $\delta\Delta$.

1. A non-trivial codeword $x \in T$ induces a subgraph Γ'.
2. By definition, Γ' must have minimum degree at least $\delta\Delta$.

Expansion and Amplification

Moral Definition: Expander graphs are graphs which *amplify* local properties into global properties.

Expander Mixing Lemma: Let $\Gamma = (V, E)$ be a Δ-regular λ-expander. Then for any $S, T \subseteq V$ we have

$$\left| E(S,T) - \frac{\Delta}{|V|}|S||T| \right| \leq \lambda\sqrt{|S||T|}. \tag{2}$$

Distance Amplification: Let $T(\Gamma, C)$ be a Tanner code with C having distance $\delta\Delta$.

1. A non-trivial codeword $x \in T$ induces a subgraph Γ'.
2. By definition, Γ' must have minimum degree at least $\delta\Delta$.
3. The EML implies the degree bound: $(\delta/2 - \lambda/\Delta)|V| \leq |V'|$.

Expansion and Amplification

Moral Definition: Expander graphs are graphs which *amplify* local properties into global properties.

Expander Mixing Lemma: Let $\Gamma = (V, E)$ be a Δ-regular λ-expander. Then for any $S, T \subseteq V$ we have

$$\left| E(S,T) - \frac{\Delta}{|V|}|S||T| \right| \leq \lambda\sqrt{|S||T|}. \tag{2}$$

Distance Amplification: Let $T(\Gamma, C)$ be a Tanner code with C having distance $\delta\Delta$.

1. A non-trivial codeword $x \in T$ induces a subgraph Γ'.
2. By definition, Γ' must have minimum degree at least $\delta\Delta$.
3. The EML implies the degree bound: $(\delta/2 - \lambda/\Delta)|V| \leq |V'|$.
4. Sufficient expansion implies $|x| \geq \delta\Delta|V'|/2 = \Theta(|E|)$.

Quantum Error Correcting Codes

A CSS Code is a type of stabilizer code where each stabilizer generator is either purely X or purely Z

Quantum Error Correcting Codes

A CSS Code is a type of stabilizer code where each stabilizer generator is either purely X or purely Z:

$$H = \begin{pmatrix} H_X & 0 \\ 0 & H_Z \end{pmatrix}. \tag{3}$$

Quantum Error Correcting Codes

A CSS Code is a type of stabilizer code where each stabilizer generator is either purely X or purely Z:

$$H = \begin{pmatrix} H_X & 0 \\ 0 & H_Z \end{pmatrix}. \tag{3}$$

The blocks H_X and H_Z define classical codes $C_X = \ker H_X$ and $C_Z = \ker H_Z$. The two codes must satisfy the CSS condition:

$$C_X^{\perp} \subseteq C_Z \iff H_Z H_X^{\mathrm{T}} = 0. \tag{4}$$

Quantum Error Correcting Codes

A CSS Code is a type of stabilizer code where each stabilizer generator is either purely X or purely Z:

$$H = \begin{pmatrix} H_X & 0 \\ 0 & H_Z \end{pmatrix}. \tag{3}$$

The blocks H_X and H_Z define classical codes $C_X = \ker H_X$ and $C_Z = \ker H_Z$. The two codes must satisfy the CSS condition:

$$C_X^{\perp} \subseteq C_Z \iff H_Z H_X^{\mathrm{T}} = 0. \tag{4}$$

The distance of the CSS code is given by

$$d_X = \min_{x \in C_Z \setminus C_X^{\perp}} |x|, \quad d_Z = \min_{x \in C_X \setminus C_Z^{\perp}} |x|, \tag{5}$$

with $d = \min(d_X, d_Z)$.

Quantum LDPC Codes

We say that a family of CSS codes is LDPC iff their constituent classical codes C_X and C_Z are LDPC.

Quantum LDPC Codes

We say that a family of CSS codes is LDPC iff their constituent classical codes C_X and C_Z are LDPC.

Difficulty with good quantum LDPC codes: $C_X^\perp \subseteq C_Z$. Tension between being low-density and being a good code.

Quantum LDPC Codes

We say that a family of CSS codes is LDPC iff their constituent classical codes C_X and C_Z are LDPC.

Difficulty with good quantum LDPC codes: $C_X^\perp \subseteq C_Z$. Tension between being low-density and being a good code.

Ingredients for a good quantum LDPC code

There must be a way to "stitch" two classical codes together to form a CSS code.

Quantum LDPC Codes

We say that a family of CSS codes is LDPC iff their constituent classical codes C_X and C_Z are LDPC.

Difficulty with good quantum LDPC codes: $C_X^\perp \subseteq C_Z$. Tension between being low-density and being a good code.

Ingredients for a good quantum LDPC code

There must be a way to "stitch" two classical codes together to form a CSS code. Global and local component.

Quantum LDPC Codes

We say that a family of CSS codes is LDPC iff their constituent classical codes C_X and C_Z are LDPC.

Difficulty with good quantum LDPC codes: $C_X^\perp \subseteq C_Z$. Tension between being low-density and being a good code.

Ingredients for a good quantum LDPC code

There must be a way to "stitch" two classical codes together to form a CSS code. Global and local component.

1. Globally, this "stitching" is accomplished using the *balanced product* [BE20]. Given two G-symmetric graphs Γ_1 and Γ_2, their balanced product is a 2-complex $\Gamma_1 \otimes_G \Gamma_2$.

Quantum LDPC Codes

We say that a family of CSS codes is LDPC iff their constituent classical codes C_X and C_Z are LDPC.

Difficulty with good quantum LDPC codes: $C_X^\perp \subseteq C_Z$. Tension between being low-density and being a good code.

Ingredients for a good quantum LDPC code

There must be a way to "stitch" two classical codes together to form a CSS code. Global and local component.

1. Globally, this "stitching" is accomplished using the *balanced product* [BE20]. Given two G-symmetric graphs Γ_1 and Γ_2, their balanced product is a 2-complex $\Gamma_1 \otimes_G \Gamma_2$.
2. Appropriate choices of local codes to ensure that the two codes compatible. This local compatibility is amplified by the expanding complex $\Gamma_1 \otimes_G \Gamma_2$ into a global compatibility.

Left-Right Cayley Complex [BE20, DELLM21]

Let G be a group. Let $A, B \subseteq G$ be two generating sets of size Δ such that $\mathrm{Cay}(A, G)$ and $\mathrm{Cay}(G, B)$ are bipartite λ-expanders.

:

Left-Right Cayley Complex [BE20, DELLM21]

Let G be a group. Let $A, B \subseteq G$ be two generating sets of size Δ such that $\mathrm{Cay}(A, G)$ and $\mathrm{Cay}(G, B)$ are bipartite λ-expanders.

The left-right Cayley complex $\mathrm{Cay}_2(A, G, B) = (Q, V, E)$ is a two-dimensional geometric complex consisting of:

Left-Right Cayley Complex [BE20, DELLM21]

Let G be a group. Let $A, B \subseteq G$ be two generating sets of size Δ such that $\mathrm{Cay}(A, G)$ and $\mathrm{Cay}(G, B)$ are bipartite λ-expanders.

The left-right Cayley complex $\mathrm{Cay}_2(A, G, B) = (Q, V, E)$ is a two-dimensional geometric complex consisting of:

1. Vertices $V = G \times \mathbb{Z}_2$.

Left-Right Cayley Complex [BE20, DELLM21]

Let G be a group. Let $A, B \subseteq G$ be two generating sets of size Δ such that $\mathrm{Cay}(A, G)$ and $\mathrm{Cay}(G, B)$ are bipartite λ-expanders.

The left-right Cayley complex $\mathrm{Cay}_2(A, G, B) = (Q, V, E)$ is a two-dimensional geometric complex consisting of:

1. Vertices $V = G \times \mathbb{Z}_2$.
2. Edges $E = E_A \sqcup E_B$ where

$$E_A = \{(g, i) \to (ag, i + 1)\} \quad \text{and} \quad E_B = \{(g, i) \to (gb, i + 1)\}.$$

Left-Right Cayley Complex [BE20, DELLM21]

Let G be a group. Let $A, B \subseteq G$ be two generating sets of size Δ such that $\mathrm{Cay}(A, G)$ and $\mathrm{Cay}(G, B)$ are bipartite λ-expanders.

The left-right Cayley complex $\mathrm{Cay}_2(A, G, B) = (Q, V, E)$ is a two-dimensional geometric complex consisting of:

1. Vertices $V = G \times \mathbb{Z}_2$.
2. Edges $E = E_A \sqcup E_B$ where

   $$E_A = \{(g, i) \to (ag, i+1)\} \quad \text{and} \quad E_B = \{(g, i) \to (gb, i+1)\}.$$

3. Faces (squares) Q, where each face $q \in Q$ is a set of four vertices of the form

   $$q = \{(g, i), (ag, i+1), (gb, i+1), (agb, i)\}.$$

Left-Right Cayley Complex [BE20, DELLM21]

Let G be a group. Let $A, B \subseteq G$ be two generating sets of size Δ such that $\mathrm{Cay}(A, G)$ and $\mathrm{Cay}(G, B)$ are bipartite λ-expanders.

The left-right Cayley complex $\mathrm{Cay}_2(A, G, B) = (Q, V, E)$ is a two-dimensional geometric complex consisting of:

1. Vertices $V = G \times \mathbb{Z}_2$.
2. Edges $E = E_A \sqcup E_B$ where

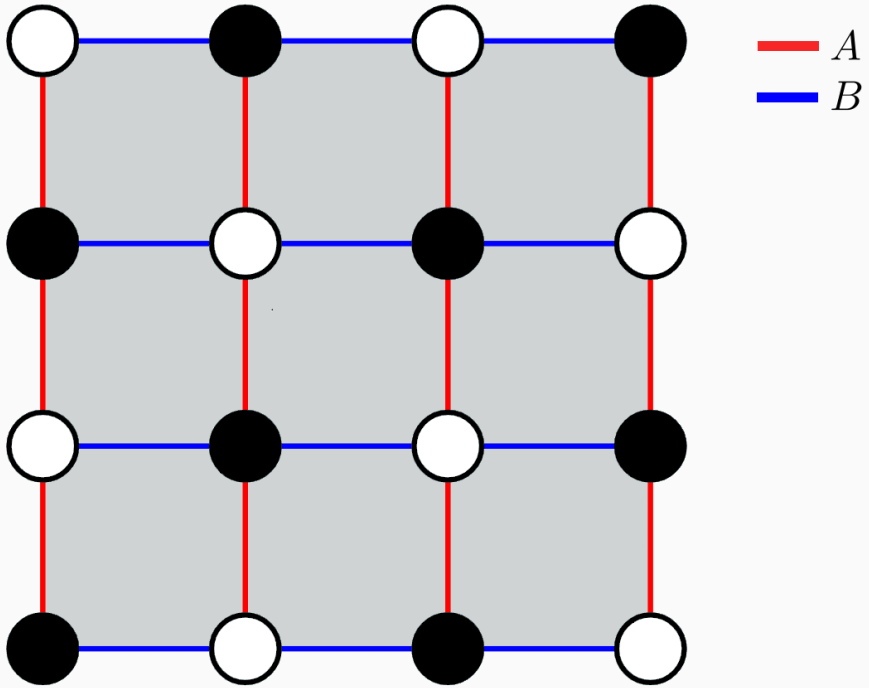
   $$E_A = \{(g, i) \to (ag, i+1)\} \quad \text{and} \quad E_B = \{(g, i) \to (gb, i+1)\}.$$

3. Faces (squares) Q, where each face $q \in Q$ is a set of four vertices of the form

   $$q = \{(g, i), (ag, i+1), (gb, i+1), (agb, i)\}.$$

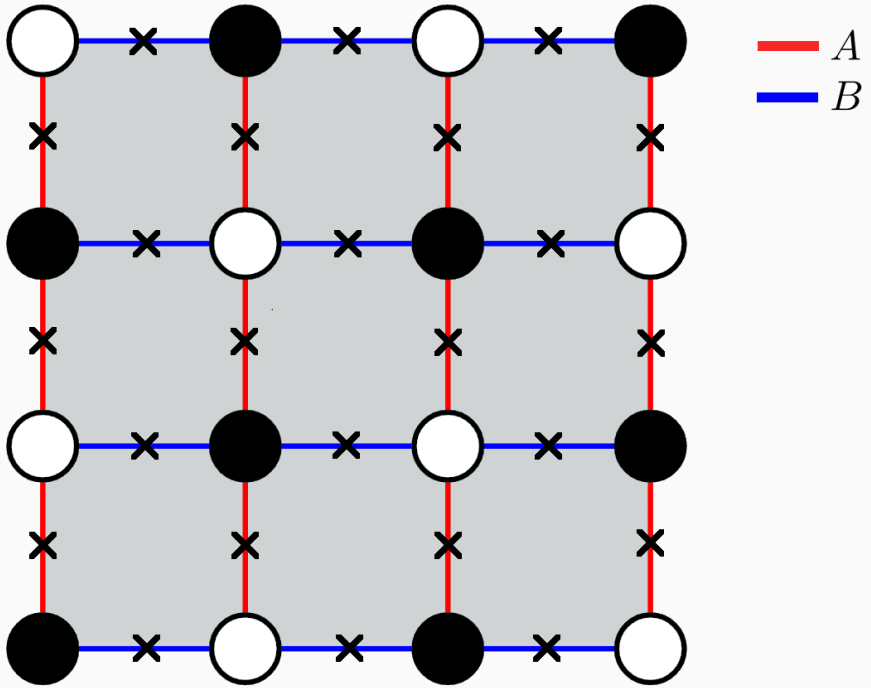
   We impose a technical restriction, called *total non-conjugacy* to ensure that faces are non-degenerate.

Quantum Tanner Codes [LZ21]



Quantum Tanner Codes [LZ21]

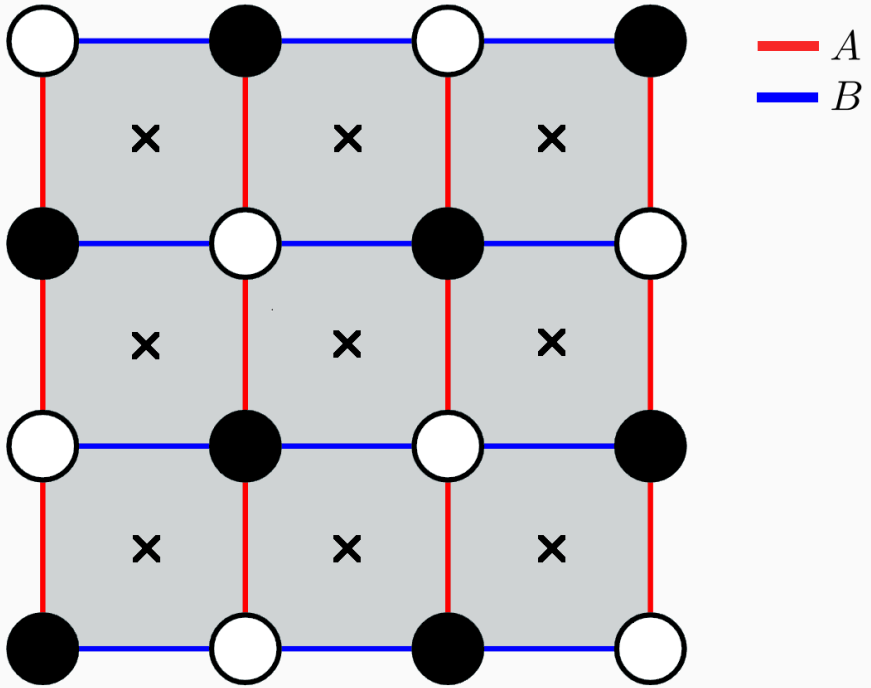
A classical Tanner code is obtained by placing bits on the edges of a graph with checks at the vertices.



Quantum Tanner Codes [LZ21]

A classical Tanner code is obtained by placing bits on the edges of a graph with checks at the vertices.

A *quantum Tanner code* is obtained by placing qubits on the *faces* of a Cayley complex with stabilizers at the vertices.

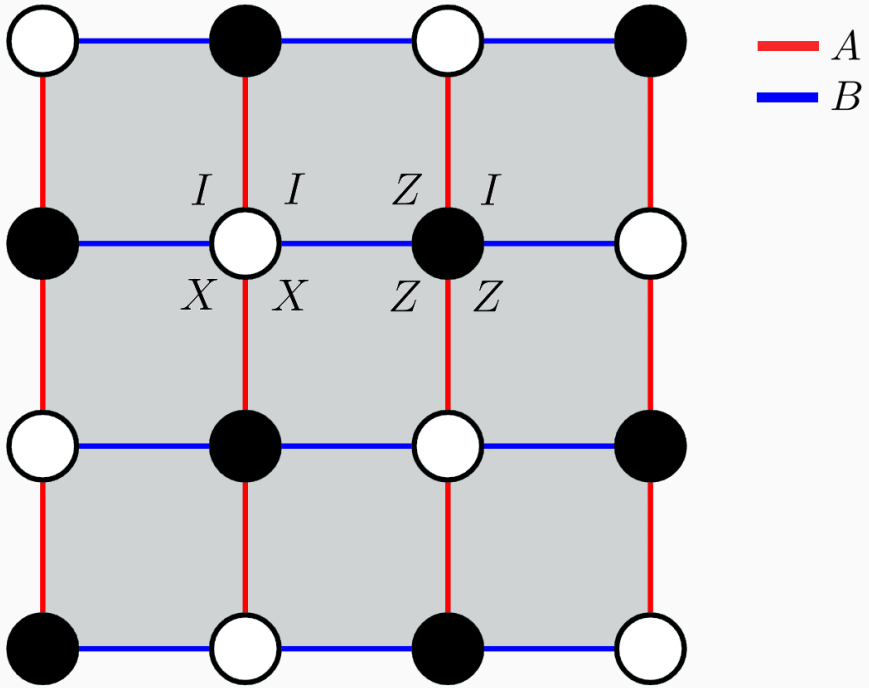


Quantum Tanner Codes [LZ21]

A classical Tanner code is obtained by placing bits on the edges of a graph with checks at the vertices.

A *quantum Tanner code* is obtained by placing qubits on the *faces* of a Cayley complex with stabilizers at the vertices.

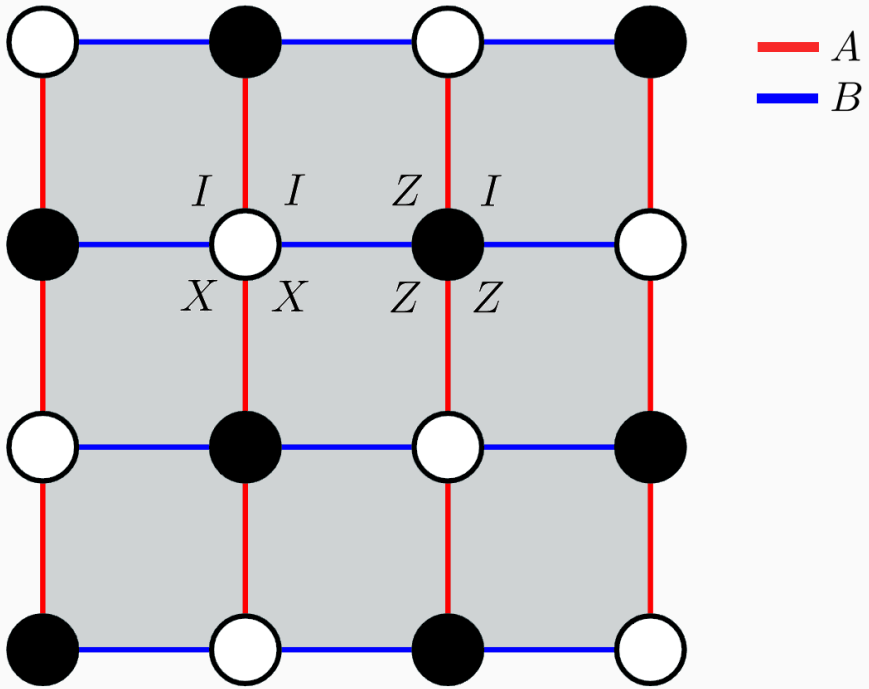
We will choose local codes C_X and C_Z such that X (resp. Z) stabilizers correspond to codewords of C_X (resp. C_Z).



Quantum Tanner Codes [LZ21]

These collection of stabilizers define a CSS code $\mathcal{C}$:

$$H = \begin{pmatrix} H_X & 0 \\ 0 & H_Z \end{pmatrix}.$$

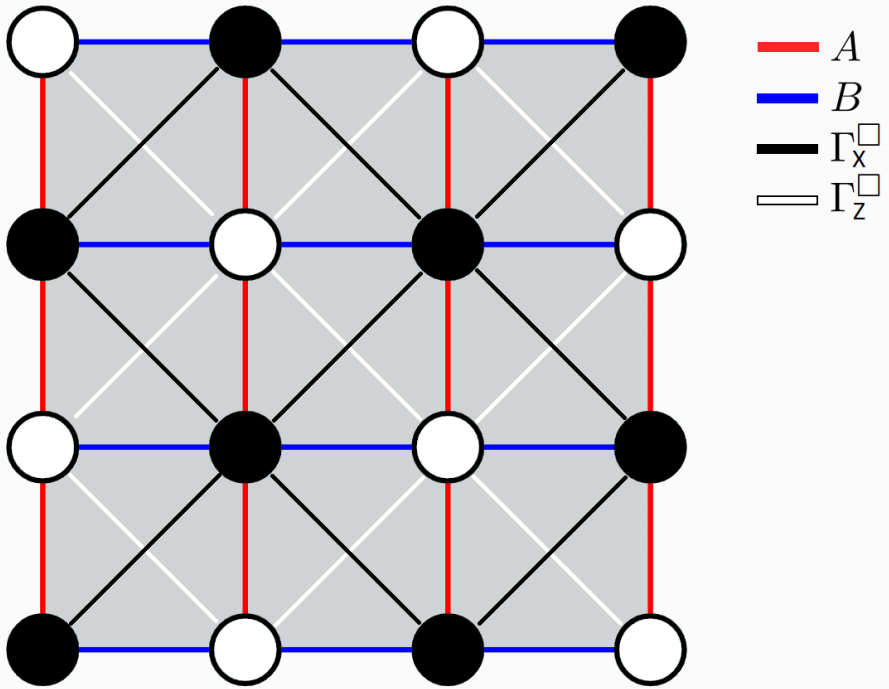


Quantum Tanner Codes [LZ21]

These collection of stabilizers define a CSS code $\mathcal{C}$:

$$H = \begin{pmatrix} H_X & 0 \\ 0 & H_Z \end{pmatrix}.$$

Introduce *face graphs* $\Gamma_X^{\square}$, $\Gamma_Z^{\square}$.



Quantum Tanner Codes [LZ21]

These collection of stabilizers define a CSS code $\mathcal{C}$:

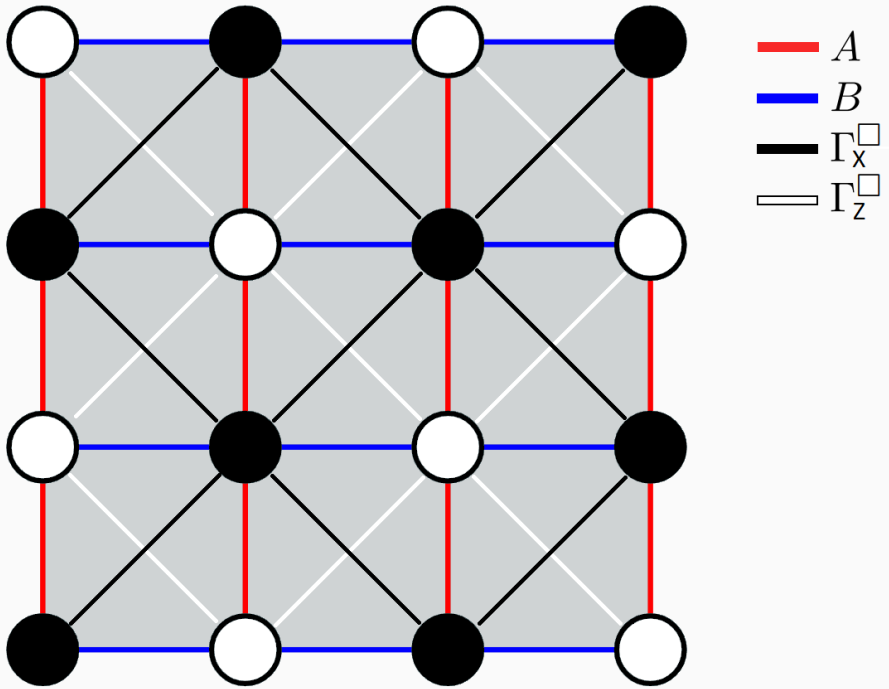
$$H = \begin{pmatrix} H_X & 0 \\ 0 & H_Z \end{pmatrix}.$$

Introduce *face graphs* $\Gamma_X^{\square}$, $\Gamma_Z^{\square}$.

Then we have

$$T_X \equiv \ker H_X = T(\Gamma_X^{\square}, C_X^{\perp}),$$
$$T_Z \equiv \ker H_Z = T(\Gamma_Z^{\square}, C_Z^{\perp}),$$

with $\mathcal{C} = \mathrm{CSS}(T_X, T_Z)$.



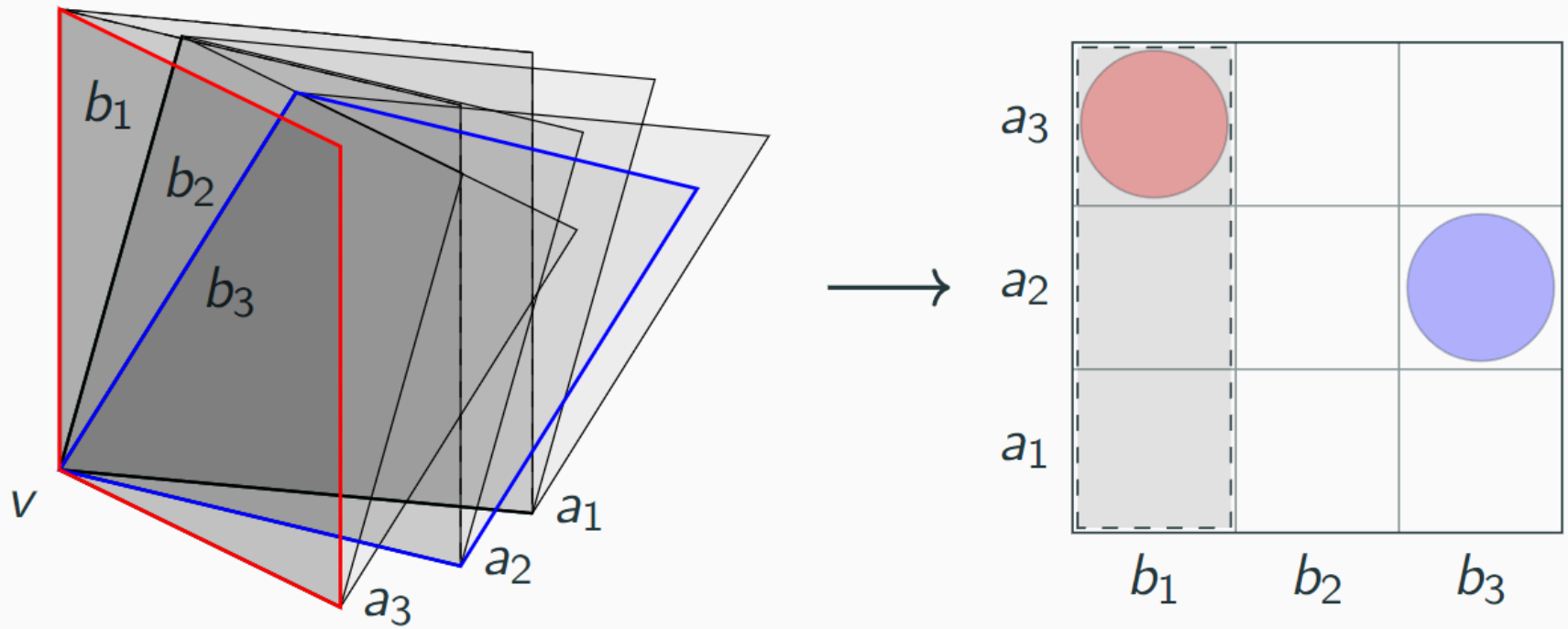
The Local View

It remains to pick the local codes C_X and C_Z.

The Local View

It remains to pick the local codes C_X and C_Z.

The local view $Q(v)$ of each vertex is in bijection with $A \times B$.
Local codewords are represented by $\Delta \times \Delta$ matrices.

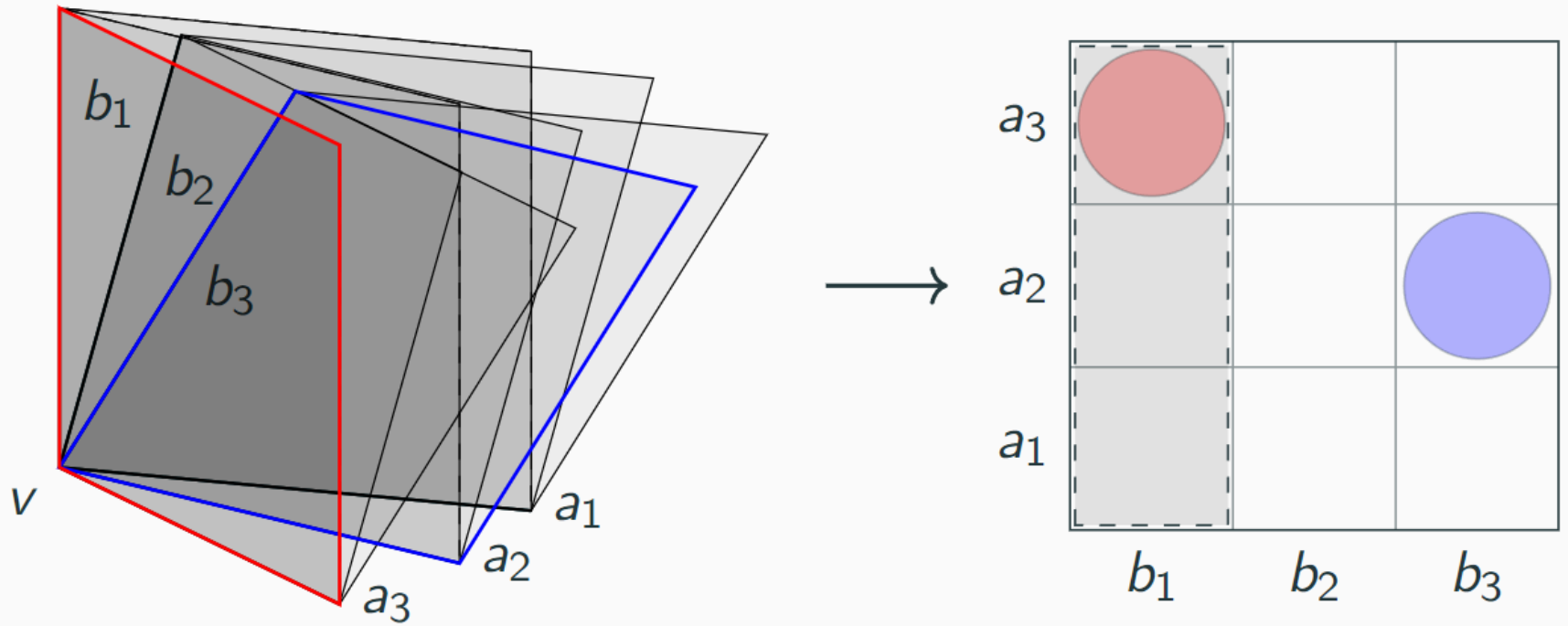


The Local View

It remains to pick the local codes C_X and C_Z.

The local view $Q(v)$ of each vertex is in bijection with $A \times B$.
Local codewords are represented by $\Delta \times \Delta$ matrices.

Convenient to pick the local codes as *tensor codes*: $C = C_1 \otimes C_2$.



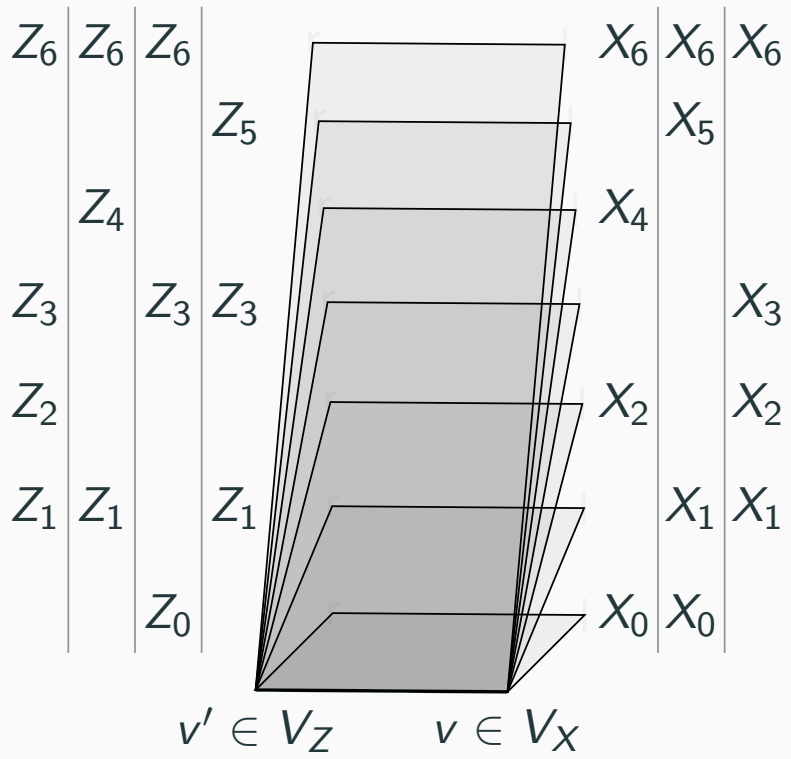
Classical Tensor Codes

Pick two classical codes $C_A \subseteq \mathbb{F}_2^A$ and $C_B \subseteq \mathbb{F}_2^B$. Let $C_Z = C_A \otimes C_B$.

Classical Tensor Codes

Pick two classical codes $C_A \subseteq \mathbb{F}_2^A$ and $C_B \subseteq \mathbb{F}_2^B$. Let $C_Z = C_A \otimes C_B$.

An X-stabilizer can overlap with a Z-stabilizer iff their anchoring vertices are adjacent. Local views coincide on a shared row or column.

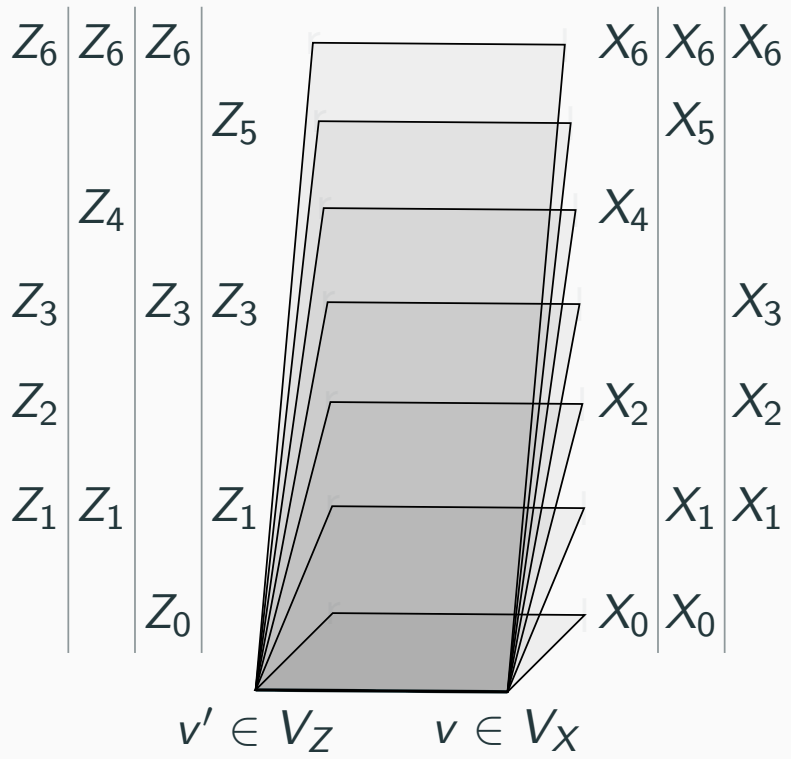


Classical Tensor Codes

Pick two classical codes $C_A \subseteq \mathbb{F}_2^A$ and $C_B \subseteq \mathbb{F}_2^B$. Let $C_Z = C_A \otimes C_B$.

An X-stabilizer can overlap with a Z-stabilizer iff their anchoring vertices are adjacent. Local views coincide on a shared row or column.

To satisfy the CSS condition, we want to choose C_X so that each row is orthogonal to C_B and each column to C_A, i.e., $C_X = C_A^\perp \otimes C_B^\perp$.



Robust Testability

Let's look at the constituent Tanner code T_X. A string $x \in \mathbb{F}_2^Q$ is a codeword for T_X iff

$$x|_{Q(v)} \in C_X^\perp = (C_A^\perp \otimes C_B^\perp)^\perp = C_A \otimes \mathbb{F}_2^B + \mathbb{F}_2^A \otimes C_B \tag{6}$$

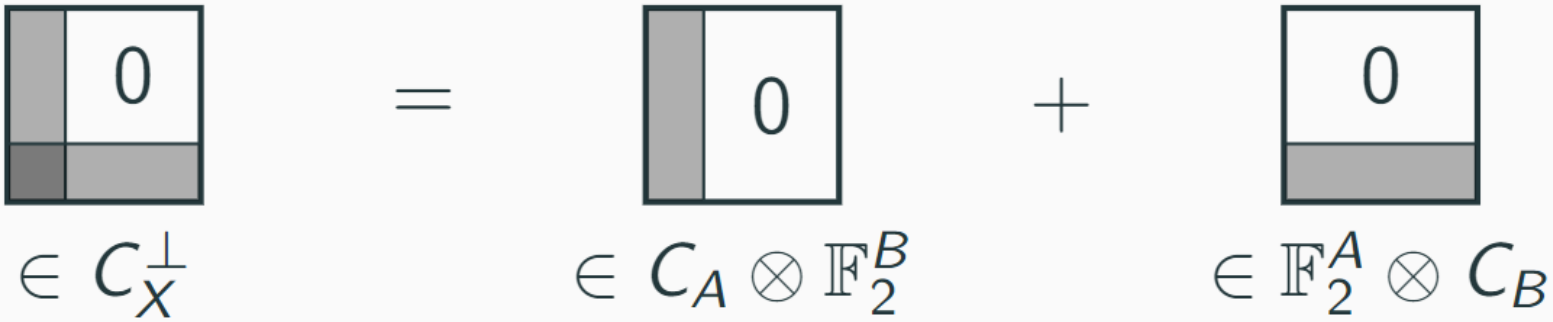
for all $v \in \Gamma_X^\square$.

Robust Testability

Let's look at the constituent Tanner code T_X. A string $x \in \mathbb{F}_2^Q$ is a codeword for T_X iff

$$x|_{Q(v)} \in C_X^\perp = (C_A^\perp \otimes C_B^\perp)^\perp = C_A \otimes \mathbb{F}_2^B + \mathbb{F}_2^A \otimes C_B \qquad (6)$$

for all $v \in \Gamma_X^\square$.

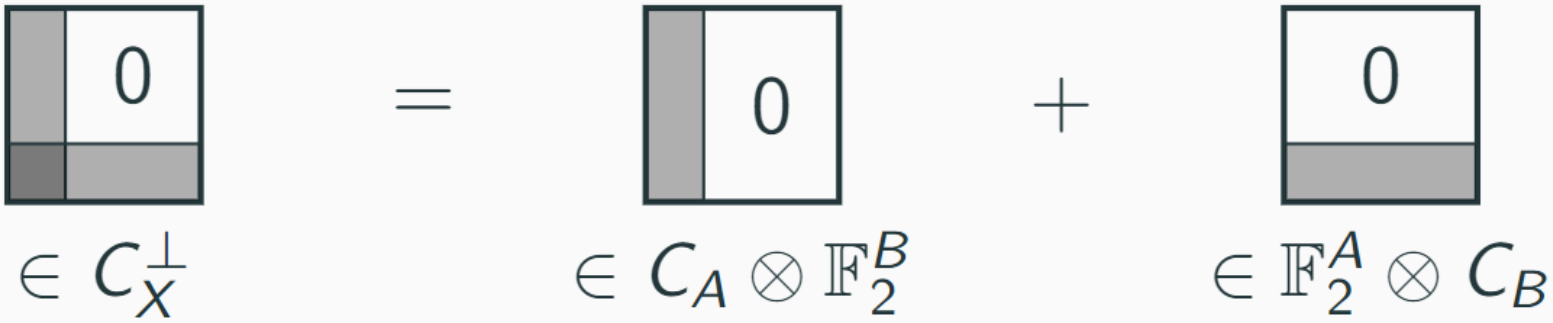


Robust Testability

Let's look at the constituent Tanner code T_X. A string $x \in \mathbb{F}_2^Q$ is a codeword for T_X iff

$$x|_{Q(v)} \in C_X^\perp = (C_A^\perp \otimes C_B^\perp)^\perp = C_A \otimes \mathbb{F}_2^B + \mathbb{F}_2^A \otimes C_B \qquad (6)$$

for all $v \in \Gamma_X^\square$.



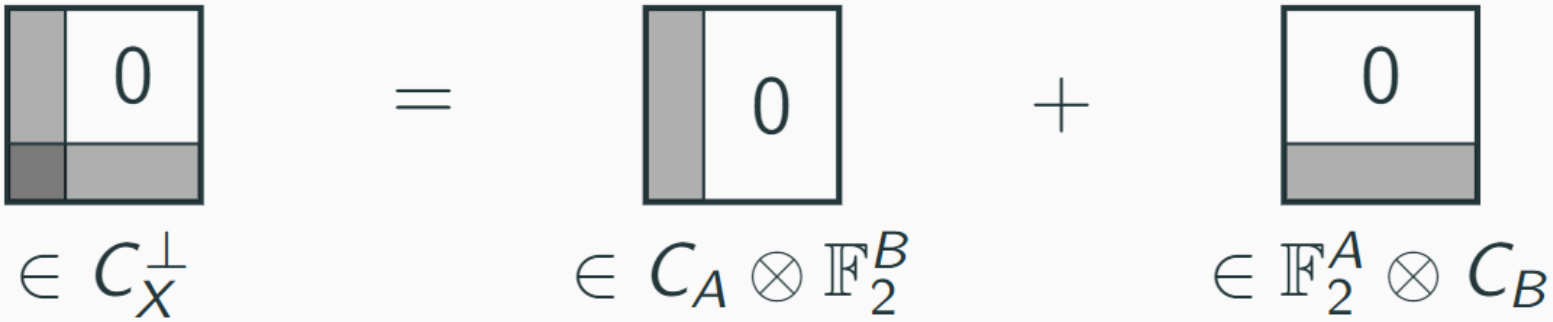
To obtain a *good* qLDPC code, a key property required is the *robust testability* of the local code.

Robust Testability

Let's look at the constituent Tanner code T_X. A string $x \in \mathbb{F}_2^Q$ is a codeword for T_X iff

$$x|_{Q(v)} \in C_X^\perp = (C_A^\perp \otimes C_B^\perp)^\perp = C_A \otimes \mathbb{F}_2^B + \mathbb{F}_2^A \otimes C_B \qquad (6)$$

for all $v \in \Gamma_X^\square$.



To obtain a *good* qLDPC code, a key property required is the *robust testability* of the local code.

Robust testability is a property of a pair of codes (C_A, C_B) saying that there cannot be "miraculous cancellations".

Robust Testability Continued

If (C_A, C_B) is robustly testable then:

Robust Testability Continued

If (C_A, C_B) is robustly testable then:

1. A sufficiently low weight codeword $x \in (C_A^\perp \otimes C_B^\perp)^\perp$ has all columns close to codewords of C_A, and all columns close to codewords of C_B.

Robust Testability Continued

If (C_A, C_B) is robustly testable then:

1. A sufficiently low weight codeword $x \in (C_A^\perp \otimes C_B^\perp)^\perp$ has all columns close to codewords of C_A, and all columns close to codewords of C_B.

2. For all $x \in \mathbb{F}_2^A \otimes \mathbb{F}_2^B$, we have

$$d(x, C_A \otimes C_B) \lesssim d(x, C_A \otimes \mathbb{F}_2^B) + d(x, \mathbb{F}_2^A \otimes C_B). \tag{7}$$

Robust Testability Continued

If (C_A, C_B) is robustly testable then:

1. A sufficiently low weight codeword $x \in (C_A^\perp \otimes C_B^\perp)^\perp$ has all columns close to codewords of C_A, and all columns close to codewords of C_B.

2. For all $x \in \mathbb{F}_2^A \otimes \mathbb{F}_2^B$, we have

$$d(x, C_A \otimes C_B) \lesssim d(x, C_A \otimes \mathbb{F}_2^B) + d(x, \mathbb{F}_2^A \otimes C_B). \qquad (7)$$

For the purposes of quantum LDPC codes, we need the stronger property of *two-sided* robust testability where both (C_A, C_B) and $(C_A^\perp, C_B^\perp)$ need to be robustly testable.

Robust Testability Continued

If (C_A, C_B) is robustly testable then:

1. A sufficiently low weight codeword $x \in (C_A^\perp \otimes C_B^\perp)^\perp$ has all columns close to codewords of C_A, and all columns close to codewords of C_B.

2. For all $x \in \mathbb{F}_2^A \otimes \mathbb{F}_2^B$, we have

$$d(x, C_A \otimes C_B) \lesssim d(x, C_A \otimes \mathbb{F}_2^B) + d(x, \mathbb{F}_2^A \otimes C_B). \tag{7}$$

For the purposes of quantum LDPC codes, we need the stronger property of *two-sided* robust testability where both (C_A, C_B) and $(C_A^\perp, C_B^\perp)$ need to be robustly testable.

A pair of independently randomly chosen codes (C_A, C_B) will be robustly testable with high probability [DHLV22, KP22].

Distance Bound

Recall minimum distance for a CSS code is

$$d_Z = \min_{x \in T_X \setminus T_Z^\perp} |x|, \quad d_X = \min_{x \in T_Z \setminus T_X^\perp} |x|. \tag{8}$$

Goal: Show any sufficiently low weight codeword is a stabilizer.

Distance Bound

Recall minimum distance for a CSS code is

$$d_Z = \min_{x \in T_X \setminus T_Z^\perp} |x|, \quad d_X = \min_{x \in T_Z \setminus T_X^\perp} |x|. \tag{8}$$

Goal: Show any sufficiently low weight codeword is a stabilizer.

Distance Sketch:

1. Consider a codeword $x \in T_X$ of sufficiently low weight.

Distance Bound

Recall minimum distance for a CSS code is

$$d_Z = \min_{x \in T_X \setminus T_Z^\perp} |x|, \quad d_X = \min_{x \in T_Z \setminus T_X^\perp} |x|. \tag{8}$$

Goal: Show any sufficiently low weight codeword is a stabilizer.

Distance Sketch:

1. Consider a codeword $x \in T_X$ of sufficiently low weight.
2. Expansion implies that there exists many local views $x|_{Q(v)}$ also with sufficiently low weight ("good" local view).

Distance Bound

Recall minimum distance for a CSS code is

$$d_Z = \min_{x \in T_X \setminus T_Z^\perp} |x|, \quad d_X = \min_{x \in T_Z \setminus T_X^\perp} |x|. \tag{8}$$

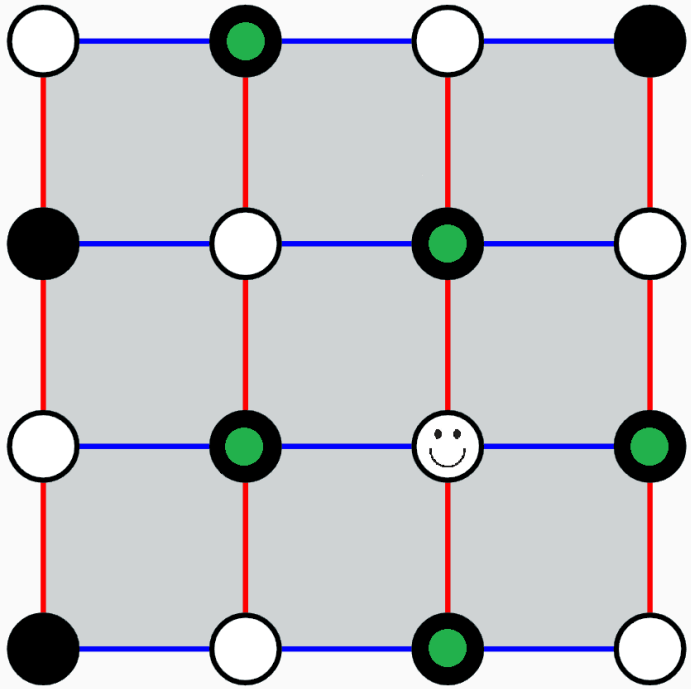
Goal: Show any sufficiently low weight codeword is a stabilizer.

Distance Sketch:

1. Consider a codeword $x \in T_X$ of sufficiently low weight.
2. Expansion implies that there exists many local views $x|_{Q(v)}$ also with sufficiently low weight ("good" local view).
3. By our previous discussion, "good" local views have rows and columns which are close to codewords of C_A and C_B.

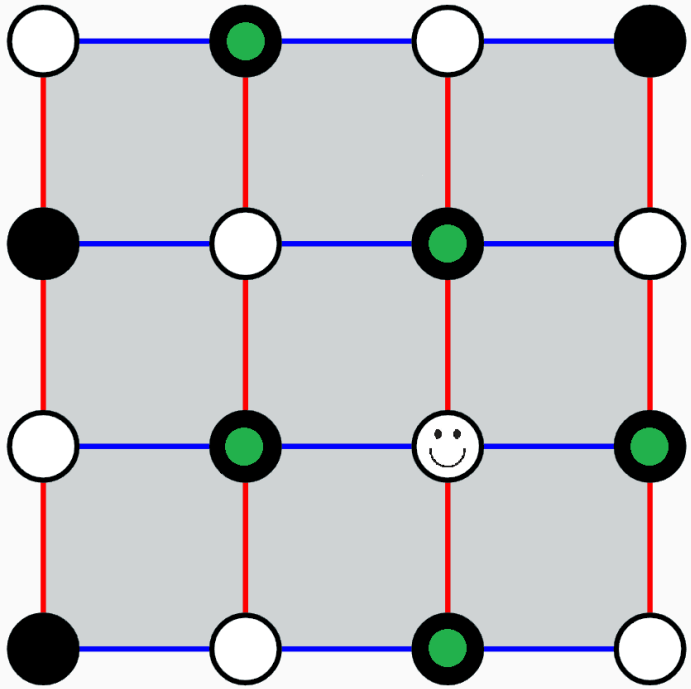
Distance Bound Sketch

4. Expansion implies that we can find a vertex $v_0 \in \Gamma_Z^{\square}$ which is adjacent to mostly "good" local views.



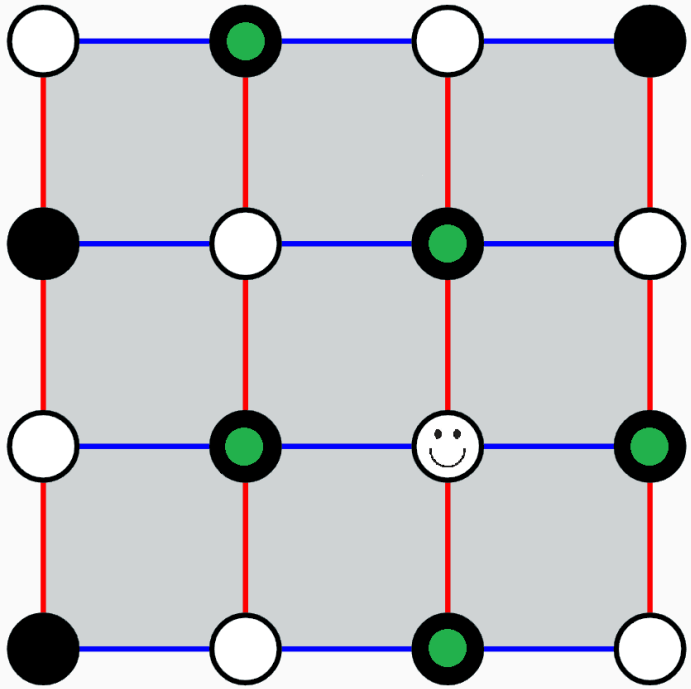
Distance Bound Sketch

4. Expansion implies that we can find a vertex $v_0 \in \Gamma_Z^{\square}$ which is adjacent to mostly "good" local views.
5. Robust testability of (C_A, C_B) implies that $x|_{Q(v_0)}$ must be close to a codeword $s \in C_A \otimes C_B$.



Distance Bound Sketch

4. Expansion implies that we can find a vertex $v_0 \in \Gamma_Z^{\square}$ which is adjacent to mostly "good" local views.
5. Robust testability of (C_A, C_B) implies that $x|_{Q(v_0)}$ must be close to a codeword $s \in C_A \otimes C_B$.
6. Iterating, it follows we can always decrease the weight of any sufficiently low weight codeword by stabilizers.



The Decoding Problem

1. Unknown Pauli error e applied to a code state.

Decoding Problem

The Decoding Problem

1. Unknown Pauli error e applied to a code state.
2. Extract syndrome $\sigma = He$ by measuring stabilizers.

Decoding Problem

The Decoding Problem

1. Unknown Pauli error e applied to a code state.
2. Extract syndrome $\sigma = He$ by measuring stabilizers.
3. Based on the syndrome σ, apply a correction f.

Decoding Problem

The Decoding Problem

1. Unknown Pauli error e applied to a code state.
2. Extract syndrome $\sigma = He$ by measuring stabilizers.
3. Based on the syndrome σ, apply a correction f.
4. Decoding succeeds if $e + f$ is a stabilizer.

Decoding Problem

The Decoding Problem

1. Unknown Pauli error e applied to a code state.
2. Extract syndrome $\sigma = He$ by measuring stabilizers.
3. Based on the syndrome σ, apply a correction f.
4. Decoding succeeds if $e + f$ is a stabilizer.

Simplifications:

1. CSS codes allow us to decode X and Z errors separately.

Decoding Problem

The Decoding Problem

1. Unknown Pauli error e applied to a code state.
2. Extract syndrome $\sigma = He$ by measuring stabilizers.
3. Based on the syndrome σ, apply a correction f.
4. Decoding succeeds if $e + f$ is a stabilizer.

Simplifications:

1. CSS codes allow us to decode X and Z errors separately.
2. Quantum Tanner codes are symmetric between X and Z.

Decoding Problem

The Decoding Problem

1. Unknown Pauli error e applied to a code state.
2. Extract syndrome $\sigma = He$ by measuring stabilizers.
3. Based on the syndrome σ, apply a correction f.
4. Decoding succeeds if $e + f$ is a stabilizer.

Simplifications:

1. CSS codes allow us to decode X and Z errors separately.
2. Quantum Tanner codes are symmetric between X and Z.

Decoding Problem for Quantum Tanner Codes

Let $e \in \mathbb{F}_2^Q$ be a X error. Given the syndrome $\sigma = H_Z e$ as input, attempt to output a correction $f \in \mathbb{F}_2^Q$ such that $e + f \in T_X^\perp$.

Decoder for Quantum Tanner Codes

Decoding Procedure:

1. Define a "potential" or "mismatch" function U which serves as a proxy for the weight of the remaining error.

Potential Function: Let $e \in \mathbb{F}_2^Q$ be an error. The *potential* of e is defined by

$$U(e) = \sum_{v \in V_Z} d\left(e|_{Q(v)}, C_Z^{\perp}\right) .$$

Decoder for Quantum Tanner Codes

Decoding Procedure:

1. Define a "potential" or "mismatch" function U which serves as a proxy for the weight of the remaining error.
2. Look for a flip-set f within the local view of a vertex which decreases U.

Potential Function: Let $e \in \mathbb{F}_2^Q$ be an error. The *potential* of e is defined by

$$U(e) = \sum_{v \in V_Z} d\left(e|_{Q(v)}, C_Z^{\perp}\right) .$$

Decoder for Quantum Tanner Codes

Decoding Procedure:

1. Define a "potential" or "mismatch" function U which serves as a proxy for the weight of the remaining error.
2. Look for a flip-set f within the local view of a vertex which decreases U.
3. If f above is found, update the error to be $e + f$ and repeat. Otherwise, output failure.

Potential Function: Let $e \in \mathbb{F}_2^Q$ be an error. The *potential* of e is defined by

$$U(e) = \sum_{v \in V_Z} d\left(e|_{Q(v)}, C_Z^{\perp}\right) .$$

The Decoding Theorem

Theorem: Let $e \in \mathbb{F}_2^Q$ be an error of weight $|e| \leq \delta n/6\Delta^{1+\varepsilon}$ with syndrome $\sigma = H_Z e$. Then there exists $v \in V$ and some $f \in \mathbb{F}_2^Q$ supported on the local view $Q(v)$, such that $U(\sigma + H_Z f) < U(\sigma)$.

The Decoding Theorem

Theorem: Let $e \in \mathbb{F}_2^Q$ be an error of weight $|e| \leq \delta n/6\Delta^{1+\varepsilon}$ with syndrome $\sigma = H_Z e$. Then there exists $v \in V$ and some $f \in \mathbb{F}_2^Q$ supported on the local view $Q(v)$, such that $U(\sigma + H_Z f) < U(\sigma)$.

Putting everything together:

Theorem [GPT22, LZ22, DHLV22]: Fix $\varepsilon > 0$, $\rho \in (0, 1/2)$, and $\delta \in (0, 1/2)$ with $\delta < h^{-1}(1-\rho)$, where $h(x)$ is the binary entropy function. For some Δ sufficiently large, there is an infinite family of quantum Tanner codes with parameters

$$[[n, k \geq (1-2\rho)^2 n, d \geq \frac{\delta}{4\Delta^{1+\varepsilon}} n]]$$

The Decoding Theorem

Theorem: Let $e \in \mathbb{F}_2^Q$ be an error of weight $|e| \leq \delta n/6\Delta^{1+\varepsilon}$ with syndrome $\sigma = H_Z e$. Then there exists $v \in V$ and some $f \in \mathbb{F}_2^Q$ supported on the local view $Q(v)$, such that $U(\sigma + H_Z f) < U(\sigma)$.

Putting everything together:

Theorem [GPT22, LZ22, DHLV22]: Fix $\varepsilon > 0$, $\rho \in (0, 1/2)$, and $\delta \in (0, 1/2)$ with $\delta < h^{-1}(1-\rho)$, where $h(x)$ is the binary entropy function. For some Δ sufficiently large, there is an infinite family of quantum Tanner codes with parameters

$$[[n, k \geq (1-2\rho)^2 n, d \geq \frac{\delta}{4\Delta^{1+\varepsilon}} n]]$$

such that for each n, there exists a $O(n)$-time decoder which can correct all errors of weight

$$|e| \leq \frac{\delta n}{14\Delta^{3+\varepsilon}}.$$

Corollary – Soundness and NLTS

Corollary (Soundness): Let e be a correctable error. Then we have

$$\Delta^2 |H_Z e| \geq U(e) \geq \Delta^{-2} d(e, T_X^{\perp}). \tag{9}$$

Corollary – Soundness and NLTS

Corollary (Soundness): Let e be a correctable error. Then we have

$$\Delta^2 |H_Z e| \geq U(e) \geq \Delta^{-2} d(e, T_X^{\perp}). \tag{9}$$

Proof: The error e can be corrected to a codeword of $T_X^{\perp}$ in at most $U(e)$ steps, and at most Δ^2 bits are flipped in each step.

Corollary – Soundness and NLTS

Corollary (Soundness): Let e be a correctable error. Then we have

$$\Delta^2 |H_Z e| \geq U(e) \geq \Delta^{-2} d(e, T_X^{\perp}). \tag{9}$$

Proof: The error e can be corrected to a codeword of $T_X^{\perp}$ in at most $U(e)$ steps, and at most Δ^2 bits are flipped in each step.

NLTS Theorem [ABN22]:

Good qLDPC CSS Code + "Clustering" $\longrightarrow$ NLTS.

Corollary – Soundness and NLTS

Corollary (Soundness): Let e be a correctable error. Then we have

$$\Delta^2 |H_Z e| \geq U(e) \geq \Delta^{-2} d(e, T_X^{\perp}). \tag{9}$$

Proof: The error e can be corrected to a codeword of $T_X^{\perp}$ in at most $U(e)$ steps, and at most Δ^2 bits are flipped in each step.

NLTS Theorem [ABN22]:

$$\text{Good qLDPC CSS Code} + \text{“Clustering”} \longrightarrow \text{NLTS}.$$

Clustering says that if a string $e \in \mathbb{F}_2^Q$ violates few checks then it must be either very high weight or very low weight.

Corollary – Soundness and NLTS

Corollary (Soundness): Let e be a correctable error. Then we have

$$\Delta^2 |H_Z e| \geq U(e) \geq \Delta^{-2} d(e, T_X^{\perp}). \tag{9}$$

Proof: The error e can be corrected to a codeword of $T_X^{\perp}$ in at most $U(e)$ steps, and at most Δ^2 bits are flipped in each step.

NLTS Theorem [ABN22]:

$$\text{Good qLDPC CSS Code} + \text{“Clustering”} \longrightarrow \text{NLTS}.$$

Clustering says that if a string $e \in \mathbb{F}_2^Q$ violates few checks then it must be either very high weight or very low weight.

This is precisely soundness, so we generally expect *efficiently decodable* good qLDPC codes to be NLTS.

Conclusions

- After ~ 20 years of progress, the $O(\sqrt{n})$ distance barrier has been broken. Improved symmetry-based products and geometric intuition.

Conclusions

- After ~ 20 years of progress, the $O(\sqrt{n})$ distance barrier has been broken. Improved symmetry-based products and geometric intuition.

- Asymptotically good quantum LDPC codes exist! Infinite families of quantum CSS codes with $O(1)$-weight stabilizers and parameters $[[n, k = \Theta(n), d = \Theta(n)]]$.

Conclusions

- After ~ 20 years of progress, the $O(\sqrt{n})$ distance barrier has been broken. Improved symmetry-based products and geometric intuition.
- Asymptotically good quantum LDPC codes exist! Infinite families of quantum CSS codes with $O(1)$-weight stabilizers and parameters $[[n, k = \Theta(n), d = \Theta(n)]]$.
- These codes are efficiently decodable (linear time, linear number of errors). Efficient quantum memories.

Conclusions

- After ~ 20 years of progress, the $O(\sqrt{n})$ distance barrier has been broken. Improved symmetry-based products and geometric intuition.
- Asymptotically good quantum LDPC codes exist! Infinite families of quantum CSS codes with $O(1)$-weight stabilizers and parameters $[[n, k = \Theta(n), d = \Theta(n)]]$.
- These codes are efficiently decodable (linear time, linear number of errors). Efficient quantum memories.
- Good quantum LDPC code + Efficient Decoder = NLTS.

References

N. Breuckmann and J. Eberhardt (2020). In: *arXiv:2012.09271*

I. Dinur et al. (2021). In: *arXiv:2111.04808*

G. Kalachev and P. Panteleev (2021). In: *arXiv:2111.03654*

A. Leverrier and G. Zémor (2022a). In: *arXiv:2202.13641*

B. Gu, C. Pattison, and E. Tang (2022). In: *arXiv:2206.06557*

A. Leverrier and G. Zémor (2022b). In: *arXiv:2206.0757*

Irit Dinur et al. (2022). In: *arXiv:2206.07750*

A. Leverrier and G. Zémor (2022c). In: *arXiv:2208.05537*